

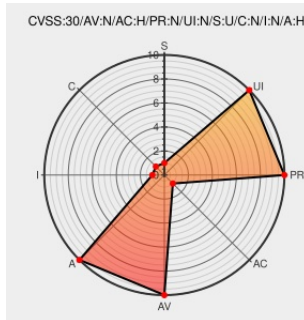


CVE-2018-14641

Published on: 09/18/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:44 PM UTC

CVE-2018-14641

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

A security flaw was found in the `ip_frag_reasm()` function in `net/ipv4/ip_fragment.c` in the Linux kernel from 4.19-rc1 to 4.19-rc3 inclusive, which can cause a later system crash in `ip_do_fragment()`. With certain non-default, but non-rare, configuration of a victim host, an attacker can trigger this crash remotely, thus leading to a remote denial-of-service.

CVE-2018-14641 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **The Linux Foundation - kernel** version **from 4.19-rc1 to 4.19-rc3 inclusive**

CVSS3 Score: **5.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **7.1 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
-------------	------	------

1629636 – (CVE-2018-14641) CVE-2018-14641 kernel: a bug in ip_frag_reasm() can cause a crash in ip_do_fragment()	Issue Tracking Patch bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-14641
oss-sec: CVE-2018-14641: Linux kernel: a security flaw in the ip_frag_reasm()	Exploit Mailing List Patch Third Party Advisory seclists.org text/html	 MLIST [oss-security] 20180918 CVE-2018-14641: Linux kernel: a security flaw in the ip_frag_reasm()
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	 CONFIRM git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=5d407b071dc369c26a38398326ee2be53651cfe4
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2018:2948

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	4.19	rc1	All	All
Operating System	Linux	Linux Kernel	4.19	rc2	All	All
Operating System	Linux	Linux Kernel	4.19	rc3	All	All
Operating System	Linux	Linux Kernel	4.19	rc1	All	All
Operating System	Linux	Linux Kernel	4.19	rc2	All	All
Operating System	Linux	Linux Kernel	4.19	rc3	All	All
cpe:2.3:o:linux:linux_kernel:4.19:rc1:*****:						
cpe:2.3:o:linux:linux_kernel:4.19:rc2:*****:						
cpe:2.3:o:linux:linux_kernel:4.19:rc3:*****:						
cpe:2.3:o:linux:linux_kernel:4.19:rc1:*****:						
cpe:2.3:o:linux:linux_kernel:4.19:rc2:*****:						
cpe:2.3:o:linux:linux_kernel:4.19:rc3:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)